FRAUD PREVENTION

Personal security means more than just protecting your physical being; it also means protecting your identity. Criminals can steal your identity by taking personal, confidential information from your mail, from your wallet, even your computer. They may overhear you giving information to someone else on the phone. Your best protection is prevention.

YOUR PERSONAL IDENTIFICATION NUMBER

Personal Identification Numbers (PIN) are used for credit cards, ATM cards, long distance calling cards, and other services.

♦ Your PIN should be memorized, secured and not given to anyone, not even family members or bank employees. The fewer people who have access to your PIN, the better.

♦ Never write your PIN on ATM or long distance calling cards. Don't write your PIN on a piece of paper and place it in your wallet.

ATM CARDS

♦ For personal safety, remove the cash as soon as the ATM releases it. Put the cash in your pocket and wait until you are in a secure location before counting it.

♦ Never use an ATM in an isolated area or where people are loitering. Avoid ATMs that have poor lighting around them.

♦ Never leave the receipt at the site. Dishonest people can use your receipt to get your account number.

♦ If you deposit money in an ATM, be sure the envelope fully drops into the machine. Never give the money to a person who promises to make the deposit for you.

Consider buying a shredder for all documents with personal information.

PROTECT YOUR MAIL

Follow these steps to make it harder for thieves to steal your mail.

♦ Never send cash or coins in the mail. Use checks or money orders.

♦ Don't leave mail in your mailbox.

♦ Have your local post office hold your mail while you are on vacation or absent from your home.

♦ If you do not receive valuable mail you are expecting, contact the issuing agency immediately.

♦ Notify your post office and others if you change your address.

♦ Always put your mail in a Postal Service mail collection box or mail slot at your local post office, or hand your mail to your letter carrier. Never place your outgoing mail in an unprotected mailbox, or into a collection box after the last scheduled pick up.

If you believe your mail has been stolen, report it immediately to your local Sheriff's Office precinct or storefront, or the Police Department.

YOUR CREDIT CARDS

- Only give your credit card account number to make a purchase or reservation that you have initiated. Never give personal information over a cellular phone.

- Watch your credit card after giving it to store clerks to protect against extra imprints being made.

- Destroy all carbons after you make a purchase (do not discard them in the trash can at the purchase counter). Keep charge slips in a safe place.

- Save all receipts, and compare them to your monthly statement. Report any discrepancies immediately!

- Keep a master list in a secure place at home with all account numbers and phone numbers for reporting stolen or lost cards. Keep another copy in a safe deposit box.

Lost or Stolen Cards

- Always report lost or stolen cards to the issuing company immediately. This limits any unauthorized use of your card and permits the company to issue a new card. Please note that protections on credit cards may not apply to debit cards. Read your cardholder agreement.

COMPUTER INFORMATION AND THE INTERNET

Increasingly, we rely on computers to store and send confidential, personal information. Like a home, computers need to be secured against intruders.

Passwords

Passwords are your first line of defense against potential computer intruders. The worst passwords to use are the ones that are obvious: your first name, spouse's name, maiden name, pets, children's name, even street addresses. The best passwords mix numbers, punctuation, and upper and lowercase letters. A password that is not found in the dictionary is even better. Programs exist that will try every word in the dictionary in an effort to crack your security.

Few people should have access to your codes and passwords. Protect your passwords by changing them regularly and memorizing them: never write them down! Never store passwords on your computer or at a web site; anyone who uses your machine will have access to information that is password protected.

Encryption: A Second Line of Defense

Encryption software "scrambles" files so they are unreadable to anyone who does not have the encryption key. Use encryption software to store important personal, financial, and security files on your computer.

Did You Really Erase That File?

Files that are deleted or erased by the user can be resurrected or recreated. Many law enforcement officials use this knowledge to fight crime; someone else could use it to commit crimes.

Do a complete "Security Erase" on your computer before you sell it or donate it. If you don't know how to do this, ask someone who does or have a shop do it for you.

Be Wary on the Internet

When you use computer, internet, or on-line services, be cautious about providing personal information. Be sure you know exactly what information about you can be accessed by other users. Finally, talk to your children and warn them never to give personal information to anyone on the Internet.